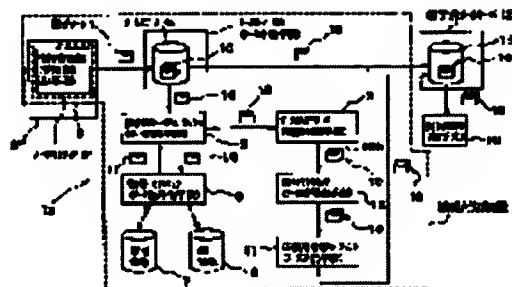


(11)Publication number : **11-252161**
(43)Date of publication of application : **17.09.1999**

HO4L 12/54
HO4L 12/58
G06F 13/00
HO4L 9/14

(71)Applicant : SEIKO EPSON CORP
(72)Inventor : HARADA MAKOTO
SHIMOMURA JUN
MIYASHITA HIROBUMI

SOLUTION: This information addition device 1 is provided with a read means 5 that reads encrypted information used to encrypt data 10 that are encrypted to be sent to a desired destination, a decoding means 6 that decodes the encrypted data 10 based on the encrypted information, an addition means 9 that adds additional information to the decoded data 10 and encryption/transmission means 11, 15 that encrypt again the data added with the additional information added to the based on the encryption information and send the result to a called party.



[Date of request for examination]	08.03.1999
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	withdrawal
[Date of final disposal for application]	25.07.2002
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

BEST AVAILABLE COPY

【特許請求の範囲】

【請求項 1】 所望の相手先に送信するために暗号化されたデータに関して、前記データを暗号化するために利用された暗号化情報を読み取る読取手段と、前記暗号化情報に基づいて、暗号化された前記データを復号化する復号化手段と、この復号化した前記データに付加情報を付加する付加手段と、

前記付加情報が付加された前記データを前記暗号化情報に基づいて再度暗号化して前記相手先に送信する暗号化／送信手段とを有することを特徴とする情報付加装置。

【請求項 2】 所望の添付情報をデータに添付して所望の相手先に暗号化された前記データを送信する際に、前記添付情報を示す識別子と、前記データを暗号化するための暗号化情報とを含むヘッダ情報を書き込む情報書込手段と、

前記ヘッダ情報が書き込まれた前記データを格納するデータ格納手段と、

前記データ格納手段に格納された前記データ中の前記ヘッダ情報から前記識別子を検出すると、前記データを前記データ格納手段から取得するデータ取得手段と、

取得した前記ヘッダ情報の前記暗号化情報を解析し、前記データを復号するデータ復号化手段と、

前記ヘッダ情報の前記識別子に基づいて、復号された前記データに対して新たな付加情報を付加する情報付加手段と、

前記付加情報が付加された前記データを前記暗号化情報に基づいて再度暗号化するためのデータ暗号化手段と、再度暗号化された前記データを前記所望の相手先に送るためのデータ送信手段とを有することを特徴とする情報付加装置。

【請求項 3】 前記情報書込手段は、前記ヘッダ情報に予め決められた相手先を書き込んで、前記データを前記データ格納手段に格納させる請求項 2 に記載の情報付加装置。

【請求項 4】 前記データは、電子メールデータである請求項 1 から 3 のいずれかに記載の情報付加装置。

【請求項 5】 暗号化されて所望の相手先に送信されるデータであり、暗号化に利用された暗号化情報が書き込まれた前記データの暗号化情報を読み取ることで前記データを一旦復号し、

前記データに所望の付加情報を付加し、

前記暗号化情報に基づき前記データを再度暗号化して前記相手先に送信することを特徴とする情報付加方法。

【請求項 6】 所望の添付情報をデータに添付して所望の相手先に暗号化された前記データを送信する際に、情報書込手段により前記添付情報を示す識別子と、暗号化された前記データの暗号化情報とを含むヘッダ情報を書き込み、

データ格納手段により前記ヘッダ情報が書き込まれた前

記データを格納し、

データ取得手段により前記データ格納手段の前記データ中に前記ヘッダ情報から前記識別子を検出すると、前記データを前記データ格納手段から取得し、前記ヘッダ情報を読み取り、

データ復号化手段により取得した前記ヘッダ情報の前記暗号化情報を解析し、前記暗号化情報に基づいて前記データを復号し、

情報付加手段により前記ヘッダ情報の前記識別子に基づいて、復号された前記データに対して新たな付加情報を付加し、

暗号化手段により前記付加情報が付加された前記データを前記暗号化情報に基づいて再度暗号化し、

データ送信手段により再度暗号化された前記データを前記所望の相手先に送信することを特徴とする情報付加方法。

【請求項 7】 前記情報書込手段は、前記ヘッダ情報に予め決められた相手先を書き込むことで、前記データを前記データ格納手段に送信して格納させる請求項 6 に記載の情報付加方法。

【請求項 8】 前記データは、電子メールデータである請求項 5 から 7 のいずれかに記載の情報付加方法。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】この発明は、ネットワークを介して転送される電子メール等のデータに所望の情報を追加する情報付加装置及び情報付加方法に関するものである。

【0002】

【従来の技術】近年、情報産業が目覚ましく発達し、電子メール等のデータ通信が、重要な情報交換手段となっている。任意の組織内のコンピュータネットワーク、パソコンネットワーク、さらには、インターネット等を経由して電子化された電子メールを交換するシステムが、多くの分野で活用されている。特に、インターネットは、標準のプロトコルである TCP/IP (Transmission Control Protocol / Internet Protocol) を採用したコンピュータ・ネットワークとして全世界をルータにより接続しており、このインターネットを介して世界中のユーザが電子メールを簡単に交換できるようになっている。このような状況の下、電子メールはその内容のセキュリティが重要視されている。このような電子メールには、暗号化方式と鍵方式とを組み合わせたセキュリティメールが採用されている。

【0003】電子メールは、RFC821 で規定されている電子メール転送のためのプロトコル SMTP (Simple Mail Transfer Protocol) により、SMTP サーバ (メールサーバ) のメールプールに一旦蓄えられる。ユーザと SMTP サーバ

とは、電子メールを読み出すときに使うプロトコル（POP3、IMAP4等）を使用し到着した電子メールが存在する場合に、電子メールを読み込む。この時、電子メールを暗号化して送信する場合も、ユーザが電子メールを暗号化し鍵方式を使って送信する。送信先のユーザは、暗号化された電子メールを受け取り、復号化をユーザの端末で行う。

【0004】

【発明が解決しようとする課題】ところが、上述のようなデータ通信においては、より利用価値のある情報を送るために、例えばメールサーバ上でこの暗号化された電子メール等に付加価値のある情報を追加して電子メール等を所望の相手先に送信したい場合がある。しかし、電子メールにて送るべきデータが既に暗号化されている場合には、新たな情報を追加したり、データの訂正を行うことができない。

【0005】この発明の目的は、上記課題を解消して、暗号化された所望の相手先に送信されるべきデータに対して、付加価値のある情報を追加することができる情報付加装置及び情報付加方法を提供することである。

【0006】

【課題を解決するための手段】請求項1の発明は、所望の相手先に送信するために暗号化されたデータに関して、前記データを暗号化するために利用された暗号化情報を読み取る読取手段と、前記暗号化情報に基づいて、暗号化された前記データを復号化する復号化手段と、この復号化した前記データに付加情報を付加する付加手段と、前記付加情報が付加された前記データを前記暗号化情報に基づいて再度暗号化して前記相手先に送信する暗号化／送信手段とを有することを特徴とする。

【0007】この請求項1の構成によれば、暗号化されて所望の相手先に送信されるデータには、データを暗号化するために必要な暗号化情報が書き込まれている。このため、この暗号化情報を読み出してデータを一旦復号化し、このデータに対して新たな付加情報を付加することができる。また、データは、暗号化情報を基にして再度暗号化されて、所望の相手先に送信される。つまり、ユーザが所望の相手先に暗号化されたデータを送信しようとした場合であっても、データに対して所望の付加情報を追加してデータを送信することができる。

【0008】請求項2の発明は、所望の添付情報をデータに添付して所望の相手先に暗号化された前記データを送信する際に、前記添付情報を示す識別子と、前記データを暗号化するための暗号化情報とを含むヘッダ情報を書き込む情報書込手段と、前記ヘッダ情報が書き込まれた前記データを格納するデータ格納手段と、前記データ格納手段に格納された前記データ中の前記ヘッダ情報から前記識別子を検出すると、前記データを前記データ格納手段から取得するデータ取得手段と、取得した前記ヘッダ情報の前記暗号化情報を解析し、前記データを復号

するデータ復号化手段と、前記ヘッダ情報の前記識別子に基づいて、復号された前記データに対して新たな付加情報を付加する情報付加手段と、前記付加情報が付加された前記データを前記暗号化情報に基づいて再度暗号化するためのデータ暗号化手段と、再度暗号化された前記データを前記所望の相手先に送るためのデータ送信手段とを有することを特徴とする。

【0009】この請求項2の構成によれば、情報書込手段は、暗号化して所望の相手先に送信したいデータに対して、追加したい付加情報を示す識別子をヘッダ情報に書き込んで、データ格納手段にデータを格納させる。データ取得手段は、データ格納手段に格納されたデータの中から、予め決められた識別子が書き込まれたヘッダ情報を発見すると、そのデータを取得する。つまり、データ取得手段は、所望のデータのみを取得することができる。データ復号化手段は、データ取得手段により取得した暗号化情報に基づいて、データを復号化することができる。そして、情報付加手段は、付加価値のある情報を付加することで、データに対して新たな付加情報を追加することができる。また、暗号化手段は、データ取得手段により取得した暗号化情報に基づいて再度暗号化してデータ送信手段によりデータを本来の送信先へと送信する。つまり、ユーザが所望の相手先に暗号化されたデータを送信しようとした場合であっても、一旦暗号化されたデータに対して、所望の付加情報を追加してデータを送信することが可能である。

【0010】請求項3の発明は、請求項2の発明において、前記情報書込手段は、前記ヘッダ情報に予め決められた相手先を書き込んで、前記データを前記データ格納手段に格納させる。

【0011】この請求項3の構成によれば、情報書込手段によりデータのヘッダ情報に予め決められた相手先を書き込んで、所定のデータ格納手段にデータを格納させることができる。これにより、データ格納手段を有する所定の相手先においてデータに所望の情報を付加することができる。また、相手先を示す識別子を変更することで、様々な場所で同様の処理を行うことができる。

【0012】請求項4の発明は、請求項1から3のいずれかの発明において、前記データは、電子メールデータである。

【0013】請求項5の発明は、暗号化されて所望の相手先に送信されるデータであり、暗号化に利用された暗号化情報が書き込まれた前記データの前記暗号化情報を読み取ることで前記データを一旦復号化し、前記データに所望の付加情報を付加し、前記暗号化情報に基づき前記データを再度暗号化して前記相手先に送信することを特徴とする。

【0014】この請求項5の構成によれば、暗号化されて所望の相手先に送信されるデータには、暗号化情報が書き込まれている。このため、この暗号化情報を読み出

してデータを一旦復号化し、このデータに対して新たな付加情報を付加することができる。また、データは、暗号化情報を基にして再度暗号化されて、所望の相手先に送信される。つまり、ユーザが所望の相手先に暗号化されたデータを送信しようとした場合であっても、データに対して所望の付加情報を追加してデータを送信することができる。

【0015】請求項6の発明は、所望の添付情報をデータに添付して所望の相手先に暗号化された前記データを送信する際に、情報書込手段により前記添付情報を示す識別子と、暗号化された前記データの暗号化情報とを含むヘッダ情報を書き込み、データ格納手段により前記ヘッダ情報が書き込まれた前記データを格納し、データ取得手段により前記データ格納手段の前記データ中に前記ヘッダ情報から前記識別子を検出すると、前記データを前記データ格納手段から取得し、前記ヘッダ情報を読み取り、データ復号化手段により取得した前記ヘッダ情報の前記暗号化情報を解析し、前記暗号化情報に基づいて前記データを復号し、情報付加手段により前記ヘッダ情報の前記識別子に基づいて、復号された前記データに対して新たな付加情報を付加し、暗号化手段により前記付加情報が付加された前記データを前記暗号化情報に基づいて再度暗号化し、データ送信手段により再度暗号化された前記データを前記所望の相手先に送信することを特徴とする。

【0016】この請求項6の構成によれば、情報書込手段は、暗号化して所望の相手先に送信したいデータに対して、追加したい付加情報を示す識別子をヘッダ情報に書き込んで、データ格納手段にデータを格納させる。データ取得手段は、データ格納手段に格納されたデータの中から、予め決められた識別子が書き込まれたヘッダ情報を発見すると、そのデータを取得する。つまり、データ取得手段は、所望のデータのみを取得することができる。データ復号化手段は、データ取得手段により取得した暗号化情報に基づいて、データを復号化することができる。そして、情報付加手段は、付加価値のある付加情報を付加することで、データに対して新たな付加情報を追加することができる。また、暗号化手段は、データ取得手段により取得した暗号化情報に基づいて再度暗号化してデータ送信手段によりデータを本来の送信先へと送信する。つまり、ユーザが所望の相手先に暗号化されたデータを送信しようとした場合であっても、一旦暗号化されたデータに対して、所望の付加情報を追加してデータを送信することが可能である。また、付加情報に様々な情報を用意することで、様々なサービスを提供することができる。

【0017】請求項7の発明は、請求項6の発明において、前記情報書込手段は、前記ヘッダ情報に予め決められた相手先を書き込むことで、前記データを前記データ格納手段に送信して格納させる。

【0018】この請求項7の構成によれば、情報書込手段によりデータのヘッダ情報に予め決められた相手先を書き込んで、所定のデータ格納手段にデータを格納させることができる。これにより、データ格納手段を有する所定の相手先においてデータに所望の情報を付加することができる。また、相手先を示す識別子を変更することで、様々な場所で同様の処理を行うことができる。

【0019】請求項8の発明は、請求項5から7のいずれかの発明において、前記データは、電子メールデータである。

【0020】

【発明の実施の形態】以下、この発明の好適な実施の形態を図面に基づいて説明する。

【0021】図1は、この発明の好ましい実施形態としての情報付加装置を一部含むデータ交換装置の一例を示す概要構成図である。

【0022】電子メールシステム（データ交換装置）1aは、ネットワークNT、送信端末STの一部を含む情報付加装置1、相手先メールサーバ12及び受信端末RT等から構成されている。

【0023】電子メールシステム1aにおいて、ネットワークNTは例えばインターネット、LAN（Local Area Network）又はWAN（Wide Area Network）等である。

【0024】情報付加装置1は、送信端末STの一部の処理、メールサーバMS、データ処理サーバ9等を有する。

【0025】送信端末STは、電子メール10（データ）を送信するための端末装置である。送信端末STは、電子メール10を送信及び／又は受信するためのソフトウェアを有する。送信端末STの詳細については、後述する。

【0026】メールサーバMSは、到着した電子メール10等を格納するためのコンピュータである。メールサーバMSは、例えばワークステーションや高性能のコンピュータである。データ処理サーバ9は、メールサーバMSに到着した電子メール10に対して、後述するように情報を付加するための処理を行うコンピュータである。メールサーバMS及びデータ処理サーバ9の詳細については、後述する。

【0027】受信端末RTは、電子メール10を受信するための端末装置である。受信端末RTは、電子メール10を送信及び／又は受信するためのソフトウェアを有する。受信端末RTの詳細については、後述する。

【0028】以上のような構成の下、電子メールシステム1aの動作の概要について説明する。

【0029】この電子メールシステム1aにおいて、送信端末STから送信された電子メール10等は、ネットワークNTを経由して所定のメールサーバMSに送信される。送信された電子メール10は、データ処理サーバ

9に送られて、詳細については後述するがデータ処理サーバ9にて所望の情報（付加情報）が付加される。そして、所望の情報を付加された電子メール10は、本来の相手先である受信端末RTのメールサーバ12に送信される。

【0030】図2は、送信端末ST、メールサーバMS、データ処理サーバ9及び受信端末RTの電気的な内部構成の概略を示すハードウェア構成図である。

【0031】送信端末ST、受信端末RTは、例えばパーソナルコンピュータ等である。以下の説明では、送信端末ST及び受信端末RTは、一例としてパーソナルコンピュータであるとして説明する。また、送信端末ST及び受信端末RTは略同様の構成を取っているため、送信端末STのみについて説明する。

【0032】送信端末STは、図2のように制御部2、通信制御部4、主記憶部3、外部記憶部7、入力部6及び表示部5を有する。

【0033】制御部2は、送信端末STにおける制御手段であり、例えばCPU（中央演算処理装置）等である。制御部2は、通信制御部4、主記憶部3、外部記憶部7、入力部6及び表示部5に接続されている。制御部2は、通信制御部4、主記憶部3、外部記憶部7、入力部6及び表示部5を制御する。

【0034】通信制御部4は、送信端末STにおけるデータ通信を行うための回路等であり、例えばパーソナルコンピュータに取り付けられたネットワークNT、モデム、携帯型の電話装置及び／又はこれらを制御するためのソフトウェア等である。

【0035】主記憶部3は、送信端末STにおける、例えばDRAM等の書き換え可能な記憶媒体である。主記憶部3は、制御部2の作業領域である。主記憶部3は、制御部2によりプログラム等を読み込むことで所定の処理を実行するためのものである。

【0036】外部記憶部7は、送信端末STにおける大容量の記録媒体であり、例えばハードディスク等である。外部記憶部7は、送信端末STにおいて記録すべき大容量の情報を格納する。入力部6は、送信端末STに対する入力を行うための入力装置であり、例えばキーボード、マウス、ポインティングデバイス及び／又はタッチパネル等である。表示部5は、送信端末STにおける表示手段であり、例えば液晶ディスプレイやブラウン管ディスプレイ等である。

【0037】メールサーバMS及びデータ処理サーバ9は、送信端末ST及び受信端末RTと略同様なハードウェア構成をしているが、メールサーバMS及びデータ処理サーバ9は高速の処理を必要とされるため、通常のパーソナルコンピュータよりも制御部2が高速であり、主記憶部3及び外部記憶部7が大容量である点が異なっている。特に、メールサーバMSにおいては、大量の電子メール10を処理するため高精度のコンピュータ等が使

用される。

【0038】図3は、図1の情報付加装置を一部に有する電子メールシステムの一例のソフトウェア構成図である。

【0039】以下の説明では、送信端末STの一部を含む情報付加装置1及び受信端末RTについて、図3及び図4等を用いてその処理内容を説明する。情報付加装置1は、予め決められた識別子を書き込まれた電子メール10に、所望の添付情報を添付して所望の相手先に暗号化して送信し、この電子メール10に対してさらに例えば付加情報を付加して相手先の送信するための装置である。以下、その詳細について説明する。

【0040】送信端末STは、電子メール10等を送信するための、例えばブラウザソフトウェア等のメールソフトウェアMP等を有する。メールソフトウェアMPは、所望の相手先である受信端末RTに対して電子メール10等を送るためのソフトウェアである。メールソフトウェアMPには、従来の電子メール10を送受信する機能に加えて、情報書き込み部3（情報書き込み手段）を有する。

【0041】電子メール10は、電子メールソフトウェアが有するメール送信機能の一部であるMIMEと呼ばれる方式により所望のファイル等のデータを添付して送信される。ここで、「MIME（Multi-Purpose Internet Mail Extension）」とは、インターネット等のネットワークにおいて、電子メールでマルチメディア関係等のデータを送るための拡張仕様を示す。このMIMEを使えば、画像データやアプリケーションソフトウェア固有のデータを電子メールの本文に埋め込んだりすることができる。

【0042】情報書き込み部3は、電子メール10のヘッダ情報10fに対して所定の内容を書き込む。電子メール10は、通常、図4（A）のように送信先10a等のヘッダ情報10f及び内容10e等から構成されている。ヘッダ情報10fは、電子メール10における内容10eの先頭に添付する情報である。電子メール10が暗号化された際には、ヘッダ情報10fの部分は暗号化されない。ヘッダ情報10fは、電子メール10の送信先を示すフィールドである送信先10a等を有する。内容10eは、電子メール10における相手先に伝えたい内容を示す部分のデータである。

【0043】情報書き込み部3は、予め設定された送信先（この実施形態では、例えばメールサーバMS）へ送信するように書き込みを行う。具体的には、情報書き込み部3は、送信先10aに書き込まれている情報を、メールサーバMSを示す識別子に書き換えを行う。この識別子は、例えばIPアドレス等である。情報書き込み部3は、図4（A）のようなヘッダ情報10fに対して、例えば図4（B）のようにXフィールド10bを作成する。Xフィールド10bは、サービスの属性10g、本

来の送信先 10b、暗号の種類 10c 及び鍵の種類 10d 等を有する。以下の実施形態の説明において、「サービス」とは、電子メール 10 に添付されたデータ等に対応した情報の区分（識別子）のことである。

【0044】サービスの属性 10g は、例えばサービスを書き込む領域である。以下の説明では、電子メール 10 に GPS (Global Positioning System) データが MIME 形式にて添付されたものとして、サービスの属性 10g に、図 4 (B) のように仮に「GPS」を書き込む。ここで、GPS とは、現在位置の経緯度等の情報を測定するシステムである。本来の送信先 10b は、予め設定された送信先へ送信されるように後述する情報書き込み部 3 により送信先 10a に書き込まれる前に元々書き込まれていた情報であって、図 4 (A) の送信先 10a の情報を書き込んで保持するための情報書き込み領域である。暗号の種類 10c は、電子メール 10 を暗号化した際の暗号化情報を書き込むための情報書き込み領域である（以下の説明では、KPS 方式を使用して暗号化したものとして、例えば「KPS」を書き込む）。鍵の種類 10d は、暗号の種類 10c 同様、鍵の種類を書き込むための情報書き込み領域である。

【0045】受信端末 RT が、送信端末 ST と異なる点は、情報書き込み部 3 は存在しない構成となっていることである。つまり、受信端末 RT は、電子メールを送受信する機能を有する通常のブラウザソフトウェアを備え、このソフトウェアを起動可能な環境を有していればよい。

【0046】情報付加装置 1 は、前述した情報書き込み手段 3 の機能に加えて、メールサーバ MS（データ格納手段）、検出用中継エージェント 5（データ取得手段）、暗号情報 7、鍵情報 8、復号ミドルウェア 6（データ復号化手段）、データ処理サーバ 9（情報付加手段）、暗号ミドルウェア 15（データ暗号化手段）及び送信用中継エージェント 11（データ送信手段）等を有する。

【0047】メールサーバ MS は、ユーザの所望の相手先に送信されることになっている電子メール 10 であって、送信端末 ST から送信された電子メール 10 をメールプール 4a に格納する。メールプール 4a は、このような電子メール 10 を多数格納することができる。メールプール 4a は、例えば外部記憶部 7 の一部の領域を使用することで電子メール 10 等のデータを格納している。

【0048】検出用中継エージェント 5 は、例えば一定時間毎に以下の検出処理を行うソフトウェアの一種である。ここで、エージェントとは、インターフェイスの一種であり、ネットワーク NT に接続された所定のコンピュータ上に自動的に実行されるソフトウェアを常駐させておき、ユーザから指令を与えることによりこのソフト

ウェアを起動して所定の処理を行うためのものである。つまり、ユーザは、エージェントを使用することで予め設定された任意のコンピュータ上で予め設定された処理を起動することを登録しておくことが可能となる。

【0049】検出用中継エージェント 5 は、メールサーバ MS に格納された電子メール 10 からそのヘッダ情報 10f のサービスの属性 10g から予め設定された情報が添付された電子メール 10 であること（例えば「GPS」と書き込まれているとする）を検出すると、その電子メール 10 を取得する。検出用中継エージェント 5 は、ヘッダ情報 10f（サービスの属性 10g（添付情報を示す識別子）、本来の送信先 10b、暗号の種類 10c（暗号化情報）及び鍵の種類 10d（暗号化情報））の内容を取得する。

【0050】現在使用されている暗号化方式は、大別すると秘密鍵暗号方式、公開鍵方式及び共有鍵方式等がある。情報付加装置 1 は、これらの暗号化方式に対応するため、予めこれらの暗号化方式に関する情報を格納する暗号情報 7 及び鍵情報 8 等を有する。

【0051】暗号情報 7 は、例えば DES、MISTY 等の暗号化と復号化に同じ鍵を使用する秘密鍵方式に関する情報を格納する。鍵情報 8 は、例えば KPS、RSA、FEAL 等のような鍵方式に関する情報を格納する。

【0052】復号ミドルウェア 6 は、暗号化された電子メール 10 を復号化するためのソフトウェアの一種である。ミドルウェアとは、例えば JAV A 等の言語で作成されたソフトウェアの部品のようなものであり、外部のアプリケーションソフトウェアからの指示により動作して使用されるものである。

【0053】復号ミドルウェア 6 は、電子メール 10 のヘッダ情報 10f に書き込まれた暗号の種類 10c（ここでは、例えば「KPS」であるとして説明する）を判別し、暗号化されたデータの復号化に関する情報を格納した暗号情報 7 及び／又は鍵情報 8 から所定の情報を取得することで、電子メール 10 を例えば KPS 方式のアルゴリズムにより復号する。

【0054】データ処理サーバ 9 は、復号ミドルウェア 6 にて暗号化された電子メール 10 に対して検出用中継エージェント 5 にて検出されたサービスの属性 10g に対応したデータ等の新たな情報（付加情報 10h）、例えば DGPS データを付加する。ここで、DGPS データとは、電子メール 10 に添付されている GPS データの位置情報を補正するための補正用 GPS データのことである。GPS データは多少の誤差を含んでいるため、DGPS データを付加することで誤差を補正する。

【0055】暗号ミドルウェア 15 は、ソフトウェアの一種である。暗号ミドルウェア 15 は、データ処理サーバ 9 にて新たな付加情報 10h を付加された電子メール 10 を暗号化する。暗号化するには、検出用中継エー

ジェント5にて検出された暗号の種類10c(例えばKPS方式)を基にして暗号化する。

【0056】送信用中継エージェント11は、暗号ミドルウェア15により暗号化された電子メール10を本来の相手先のメールサーバ12に送信するために、電子メール10の形式を図4(C)のように送信先10aに本来の送信先10bに書き込まれていた情報を元へ戻すように書き込む処理を行う。

【0057】この発明の好ましい実施形態としての情報付加装置は、以上のような構成であり、次にその動作について説明する。

【0058】図5は、図1の電子メールシステム1aの一部としての情報付加方法の処理手順の一例を示すフローチャートである。

【0059】〈送信端末ST側での処理(ステップST1~4)〉ユーザは、メールソフトウェアMPを使用して電子メール10を所望の相手に送信する際に、例えばMIME形式にて所望の情報を添付する(ステップST1)。そして、ユーザは、電子メール10を所望の相手先に送信する。この時、電子メール10は、暗号化されて送信される(ステップST2)。また、同時に情報書き込み部3は、電子メール10に前述したように所定の宛先(例えば、メールサーバMS)に到着する等のようにしたり、電子メール10を暗号化する際の暗号化情報を認識可能としたり、所定の識別子を認識可能とするためにヘッダ情報10fを書き込む(ステップST3)。このような処理を行った後、メールソフトウェアMPのメール送信機能によりメールサーバMSに対して送信する(ステップST4)。

【0060】〈メールサーバMS等側での処理(ステップST5~10)〉メールソフトウェアMPのメール送信機能によりメールサーバMSに対して送信された電子メール10は、メールサーバMSの格納部4へ格納されている。検出用中継エージェント5は、メールサーバMSに到着した電子メール10のヘッダ情報10fを例えば一定時間毎に検出する(ステップST5)。

【0061】もし、このヘッダ情報10fのXフィールド10bに書き込まれたサービスの属性10gが存在しない場合等であって、検出用中継エージェント5により付加情報10hを電子メール10に付加する必定がないと判別されると(ステップST6)、ステップST10に進み、メールサーバMSは、直接電子メール10を本来の相手先である受信端末RTのメールサーバ12に送信する(ステップST10)。

【0062】一方、ヘッダ情報10fのXフィールド10bに書き込まれたサービスの属性10gが存在する場合等では、検出用中継エージェント5が読み出したヘッダ情報10fの暗号の種類10cから、復号ミドルウェア6が前述したように暗号化された電子メール10を復号化する(ステップST7)。復号化された電子メール

10は、データ処理サーバ9によりサービスの属性10gに基づいた付加情報10hを電子メール10に付加する(ステップST8)。そして、電子メール10は、検出用中継エージェント5が読み出したヘッダ情報10fの暗号の種類10cを基にして、暗号ミドルウェア15により再度暗号化される(ステップST9)。そして、送信用中継エージェント11は、電子メール10を相手先のメールサーバ12に送信する(ステップST10)。

【0063】このようにして、相手先のメールサーバ12に送信された電子メール10は、POP3又はIMAP4等のプロトコルを使用して、受信端末RTにより取得される。POP3等は、メールサーバ12に到着した電子メール10を、受信端末RTが取り込めるようにするためのプロトコルである。

【0064】以上のようにして、暗号化されて所望の相手先に送信される電子メール10には、暗号化情報が書き込まれている。このため、この暗号化情報を読み出して電子メール10を一旦復号化し、この電子メール10に対して新たな付加情報を付加することができる。また、電子メール10は、暗号化情報を基にして再度暗号化されて、所望の相手先に送信される。つまり、ユーザが所望の相手先に暗号化された電子メール10を送信しようとした場合であっても、電子メール10に対して所望の付加情報を追加して電子メール10を送信することができる。

【0065】この発明は、上記実施の形態に限定されず、特許請求の範囲を逸脱しない範囲で種々の変更を行うことができる。

【0066】電子メール等のデータに付加する情報の例としては、例えば、以下のようなものがある。

【0067】電子メール10に対して、プレゼントを相手先に送りたい旨をヘッダ情報10fに書き込んで送信することにより、情報付加装置1にてクレジット番号を付加する。これにより、プレゼントの代金をクレジット番号に基づいて自動的に支払うことができる。

【0068】また、この発明の好ましい実施形態では、各処理が各コンピュータに分散されて配置しているが、各処理について一部又は全体をまとめた形態でも良いことはいうまでもない。

【0069】

【発明の効果】この請求項1及び5の発明によれば、それぞれ暗号化されたデータであって、所望の相手先に送信されるべきデータに対して、付加価値のある情報を追加することができる。付加する情報としてさらに様々な付加情報を用意してデータに付加することで、様々なサービスを提供することができる。

【0070】この請求項2及び6の発明によれば、それぞれ暗号化されたデータであって、所望の相手先に送信されるべきデータに対して、付加価値のある情報を追加

することができる。この際、データに書き込まれた添付情報を示す識別子を判別することで、この添付情報に対応する付加情報をデータに添付することが可能である。また、付加する情報として様々な情報を用意してデータに付加することで、様々なサービスを提供することができる。

【0071】この請求項3及び7の発明によれば、それぞれデータ格納手段を有する所定の相手先においてデータに所望の付加情報を追加することができる。従って、相手先を示す識別子を設定することで、様々な場所で付加情報を追加することができる。

【0072】この請求項4及び8の発明によれば、それぞれ今日、目覚ましく発達した情報産業において、電子メール等による情報交換に新しいサービスを提供することができる。

【図面の簡単な説明】

【図1】この発明の好ましい実施形態としての情報付加装置を含むデータ交換装置を示す概要構成図。

【図2】図1の送信端末、受信端末、データ処理サーバ及びメールサーバ等の内部構成の概略を示すハードウェア構成図。

【図3】図1の情報付加装置を一部に有するデータ交換装置の処理手順の一例を示すソフトウェア構成図。

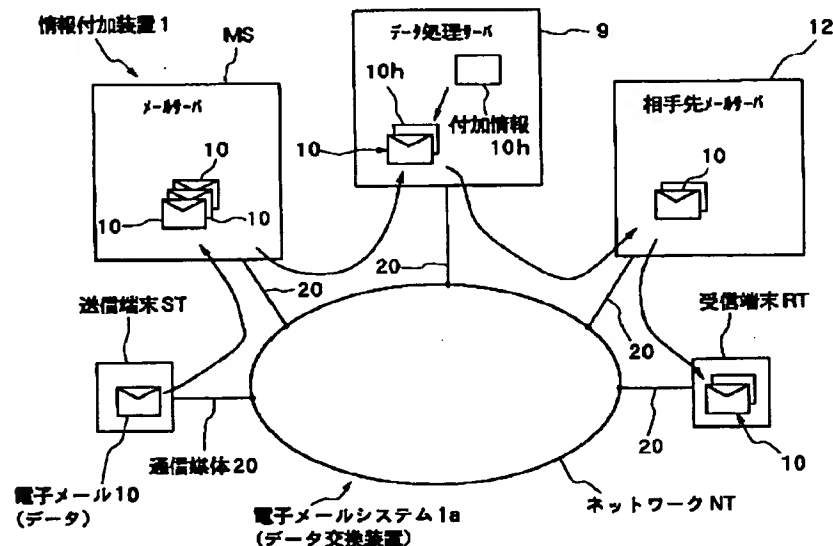
【図4】図1のデータの一例としての電子メールのデータ形式を示すフォーマット。

【図5】図1の情報付加装置における情報付加方法の処理手順の一例を示すフローチャート。

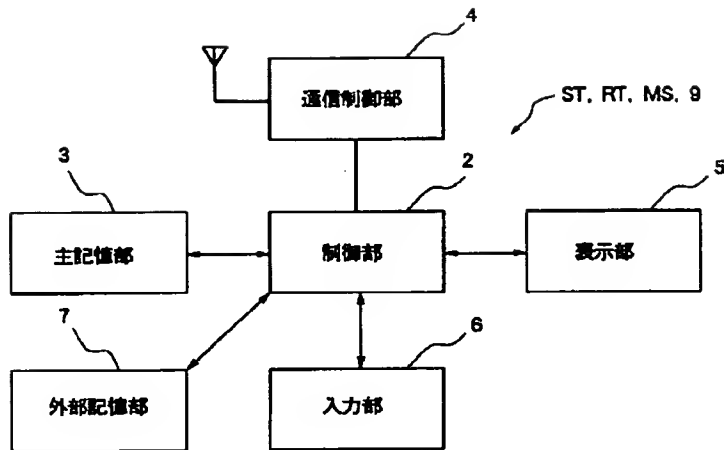
【符号の説明】

- 1 情報付加装置
- 1a 電子メールシステム（データ交換装置）
- 3 情報書き込み部（情報書き込み手段）
- 4 メールサーバ（データ格納手段）
- 5 検出用中継エージェント（データ取得手段、読取手段）
- 6 復号ミドルウェア（データ復号手段、復号化手段）
- 9 データ処理サーバ（情報付加手段、付加手段）
- 10 電子メール（データ）
- 10h 付加情報
- 11 送信用中継エージェント（データ送信手段、暗号化／送信手段）
- 15 暗号ミドルウェア（データ暗号手段、暗号化／送信手段）
- ST 送信端末
- RT 受信端末（所望の相手先）

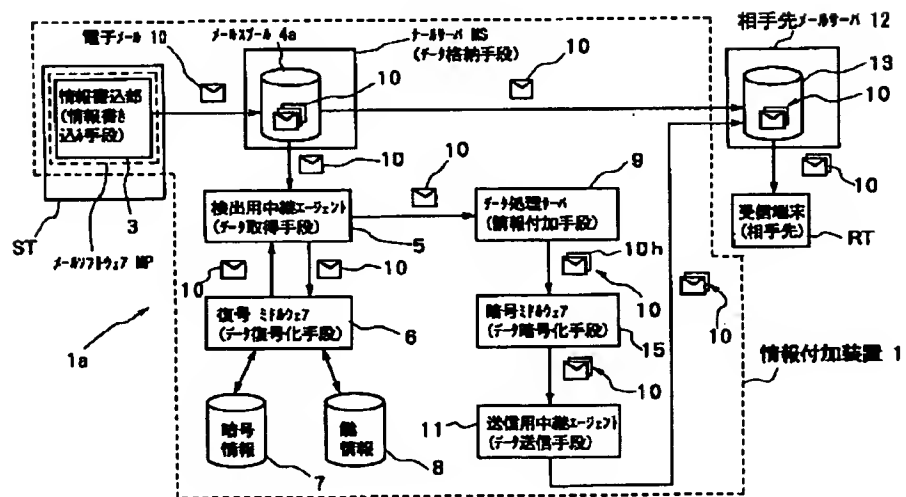
【図1】



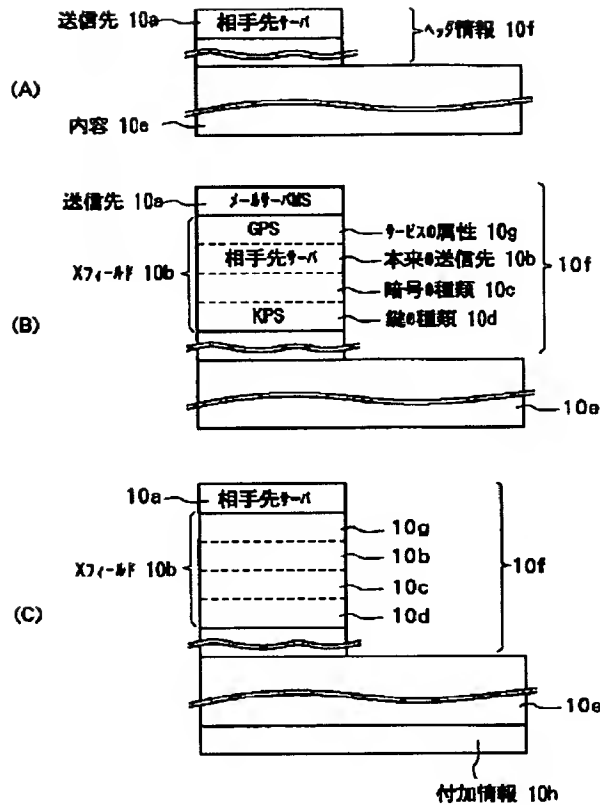
【図 2】



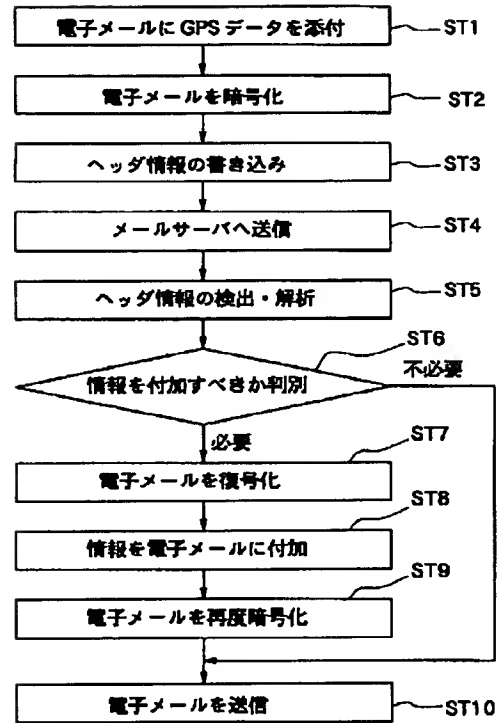
【図 3】



【図 4】



【図 5】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.